500.36158CX1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Y. SAITO, et al

Serial No.: Not yet assigned

Filed: June 4, 2001

For: SECURITY MANAGEMENT METHOD FOR NETWORK SYSTEM

Group: 2182

Examiner: N. Nguyen

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

June 4, 2001

Sir:

The following amendments and remarks are respectfully submitted prior to the Rule 53(b) Continuation Application filed on even date.

IN THE SPECIFICATION

Please insert before the first line of the specification the following:

-- This is a continuation of application Serial No. 09/048,986, filed March 27, 1998. --

IN THE CLAIMS

Please cancel claims 1-15 without prejudice or disclaimer of the subject matter thereof.

Please add new claims 16-24 as follows:

-- 16. A method for performing authentication between a client and a service server connected over a network, comprising the steps of:

generating, by said client, a random number, ciphering said random number, and transmitting said random number thus ciphered to said service server;

deciphering, by said service server, said ciphered random number transmitted from said client, re-ciphering said random number thus deciphered, and transmitting said random number thus re-ciphered to said client; and

re-deciphering, by said client, said re-ciphered random number, confirming whether said random number thus re-deciphered coincides with said random number generated by said client, and sending an inquiry about start of a service to said service server based on a result of the confirmation about said random number.

17. The method according to claim 16, wherein when re-ciphering said deciphered random number, said service server not only re-ciphers said deciphered random number but also ciphers a code indicating said service server, and transmits said re-ciphered random number and said code thus ciphered to said client; and

when re-deciphering said re-ciphered random number, said client not only re-deciphers aid re-ciphered random number but also deciphers aid ciphered code, confirms whether a service server which transmitted said re-ciphered random number and said ciphered code coincides with said service server to which said client transmitted said ciphered random number, and sending said inquiry about start of said service to said service server, based on a result of the confirmation about said service server.

18. A computer program for use in performing authentication between a client and a service server connected over a network, comprising the steps of:

generating, by said client, a random number, ciphering said random number, and transmitting said random number thus ciphered to said service server;

deciphering, by said service server, said ciphered random number transmitted from said client, re-ciphering said random number thus deciphered, and transmitting said random number thus re-ciphered to said client; and

re-ciphering, by said client, said re-ciphered random number, confirming whether said random number thus re-deciphered coincides with said random number generated by said client, and sending an inquiry about start of a service to

said service server based on a result of the confirmation about said random number.

19. An authentication system comprising:

a client; and

a service server connected over a network,

wherein said client generates a random number, ciphers said random number, and transmits said random number thus ciphered to said service server,

wherein said service server deciphers said ciphered random number, re-ciphers said random number thus deciphered, and transmits said random number thus re-ciphered to said client, and

wherein said client re-deciphers said re-ciphered random number, confirms whether said random number thus re-deciphered coincides with said random number generated by said client, and sends an inquiry about start of a service to said service server based on a result of the confirmation about said random number.

20. A method for performing authentication between a first computer and a second computer connected over a network, comprising the steps of:

transmitting, by said first computer, a service request to said second computer, a certificate being attached to said service request;

generating, by said second computer, a ciphering key according to a result of confirmation of said certificate transmitted from said first computer, ciphering said ciphering key with a public key of said first computer, and transmitting said ciphering key thus ciphered to said first computer;

generating, by said first computer, a random number, deciphering said ciphered ciphering key, ciphering said random number with said ciphering key thus deciphered, and transmitting said random number thus ciphered to said second computer;

deciphering, by said second computer, said ciphered random number, re-ciphering said random number thus deciphered and ciphering a code indicating said second computer both using a private code of said second computer, and transmitting said random number thus re-ciphered and said code thus ciphered to said first computer; and

re-deciphering, by said first computer, said re-ciphered random number and deciphering said ciphered code both using a public key of said second computer, confirming whether said re-deciphered random number coincides with said random number generated by said first computer and whether said code thus deciphered is valid, and sending an inquiry about start

of a service based on results of the confirmation about said random number and the confirmation about said code.

21. The method according to claim 20, wherein said ciphering key is a session key.

22. The method according to claim 20, wherein said code indicating said second computer is either one of a name of said second computer and a certificate of said second computer.

23. A computer program for use in performing authentication between a first computer and a second computer connected over a network, comprising the steps of:

transmitting, by said first computer, a service request to said second computer, a certificate being attached to said service request;

generating, by said second computer, a ciphering key according to a result of confirmation of said certificate transmitted from said first computer, ciphering said ciphering key with a public key of said first computer, and transmitting said ciphering key thus ciphered to said first computer;

generating, by said first computer, a random number, deciphering said ciphered ciphering key, ciphering said random number with said ciphering key thus deciphered, and

transmitting said random number thus ciphered to said second computer;

deciphering, by said second computer, said ciphered random number, re-ciphering said random number thus deciphered and ciphering a code indicating said second computer both using a private code of said second computer, and transmitting said random number thus re-ciphered and said code thus ciphered to said first computer; and

re-deciphering, by said first computer, said re-ciphered random number and deciphering said ciphered code both using a public key of said second computer, confirming whether said re-deciphered random number coincides with said random number generated by said first computer and whether said code thus deciphered is valid, and sending an inquiry about start of a service based on results of the confirmation about said random number and the confirmation about said code.

24. An authentication system comprising:

a first computer; and

a second computer connected over a network,

wherein said first computer transmits a service request to said second computer, a certificate being attached to said service request,

wherein said second computer generates a ciphering key according to a result of confirmation of said certificate

transmitted from said first computer, ciphers said ciphering key with a public key of said first computer, and transmits said ciphering key thus ciphered to said first computer,

wherein said first computer generates a random number, deciphers said ciphered ciphering key, ciphers said random number with said ciphering key thus deciphered, and transmits said random number thus ciphered to said second computer,

wherein said second computer deciphers said ciphered random number, re-ciphers said random number thus deciphered and ciphers a code indicating said second computer both using a private code of said second computer, and transmits said random number thus re-ciphered and said code thus ciphered to said first computer, and

wherein said first computer re-deciphers said re-ciphered random number and deciphers said ciphered code both using a public key of said second computer, confirms whether said re-deciphered random number coincides with said random number generated by said first computer and whether said code thus deciphered is valid, and sends an inquiry about start of a service based on results of the confirmation about said random number and the confirmation about said code.--

IN THE ABSTRACT

Please replace the Abstract with the attached new Abstract.

REMARKS

Entry of the above amendments prior to examination is respectfully requested.

Please charge any shortage in fees due in connection with the filing of this paper, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (50.36158CX1).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 312-6600

ABSTRACT

A plurality of application servers, a client, an integrated authentication server and a security information management server are connected to a network. A user having different combinations of user ID's and passwords or certificates for different services processed by the application servers makes requests for services thought the client using a common integrated certificate. An application server receiving the integrated certificate transfers it to the integrated authentication server. The integrated authentication server checks information of the security information management server to decide whether the right of the user to access the service is valid and when valid, transmits to the application server a combination of a user ID and a password or a certificate. The application server performs user authentication for the user based on the combination of user ID and password or certificate.